

AMENDMENTS TO THE CLAIMS

1. (Currently Amended) A method for detecting abnormal traffic at a network level using a statistical analysis, the method comprising the steps of:

a) gathering local traffic data from each network device and integrating a plurality of the local traffic data to generate traffic data for approximating in the an overall network traffic level by a single traffic sensing module;

b) extracting a characteristic network traffic data ~~based on~~ corresponding to the traffic data in the overall network traffic level;

c) comparing the characteristic network traffic data with a predetermined characteristic network traffic data profile resulting from statistical computations and representing normal traffic, and determining whether there is abnormal traffic ~~in at~~ the network level;

d) updating the predetermined characteristic traffic data profile using the characteristic traffic data if there is no abnormal traffic in the network, and analyzing a volume amount of the abnormal traffic and monitoring the abnormal traffic if there is abnormal traffic ~~in at~~ the network level; and

e) transmitting the analysis result of the volume amount of the abnormal traffic to an abnormal traffic processing system to detect abnormal traffic without operation of a network manager, and processing the abnormal traffic to prevent a network failure.

2. (Original) The method as recited in claim 1, wherein the characteristic traffic data includes:

information on traffic assigned to an application port which is selected according to an application service;

information on traffic of which packet size is identical; and

information on traffic of which the number of source-destination pairs, which represents the number of source addresses of the traffic having the same target address.

3. (Cancelled)

4. (Currently Amended) A computer-readable recording medium for storing a program that implements a method for detecting abnormal traffic at a network level using a statistical analysis, the method comprising the steps of:

a) gathering local traffic data from each network device and integrating a plurality of the local traffic data to generate traffic data for approximating in the an overall network traffic level by a single traffic sensing module;

b) extracting a characteristic network traffic data ~~based on~~ corresponding to the traffic data in the overall network traffic level;

c) comparing the characteristic network traffic data with a predetermined characteristic network traffic data profile resulting from statistical computations and representing normal traffic, and determining whether there is abnormal traffic ~~in at~~ the network level;

d) updating the predetermined characteristic traffic data profile using the characteristic traffic data if there is no abnormal traffic in the network, and analyzing a volume amount of the abnormal traffic and monitoring the abnormal traffic if there is abnormal traffic ~~in at~~ the network level; and

e) transmitting the analysis result of the volume amount of the abnormal traffic to an abnormal traffic processing system to detect abnormal traffic without operation of a network manager, and processing the abnormal traffic to prevent a network failure.